PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-240826

(43)Date of publication of application : 11.09.1998

(51)Int.Cl. G06F 17/60

G09C 1/00

H04L 9/08

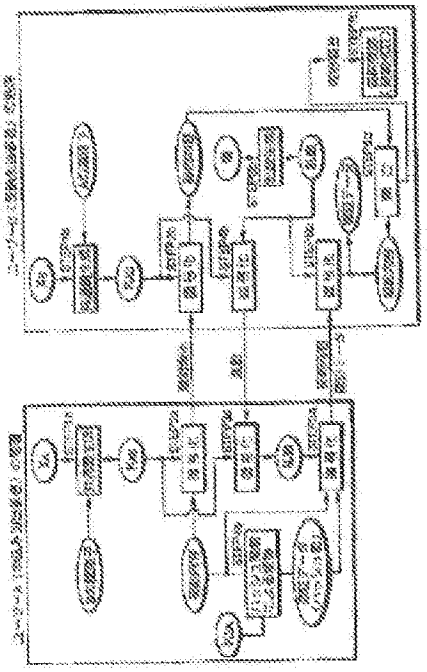
(21)Application number : 09-047962

(22)Date of filing : 03.03.1997

(71)Applicant : CARD KOOLE SERVICE KK

(72)Inventor : BABA YOSHIMI

(54) ELECTRONIC CONTRACTING METHOD



(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic contracting method for constructing a simple and prevailing electronic contracting system in which cipher communication using a common key can be operated, and the reliability of contract can be improved between persons concerned.

SOLUTION: When a user B receives the indication of the intention of the conclusion of contract from a user A, the user B generates a random number using one generative number as a seed by its own terminal equipment, enciphers it by a common key KAB with the user A, and transmits it to the user A. The user A decodes the random number by the common KAB, enciphers a contract content by using the random number as a key, transmits it to the user B, and applies for contract to the user B. Moreover, the user A transmits certification data obtained by converting the contract content by a hash function decided by its own secret key KSA to the user B.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－240826

(43)公開日　平成10年(1998)９月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ｚ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ａ
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/21	３３０
		Ｈ０４Ｌ　9/00	６０１Ｄ

審査請求　未請求　請求項の数13　ＯＬ　（全 15 頁）

(21)出願番号　特願平9－47962

(22)出願日　平成９年(1997)３月３日

(71)出願人　595095135
カード・コール・サービス株式会社
東京都渋谷区道玄坂１丁目22番７号
(72)発明者　馬場　芳美
千葉県船橋市宮本８丁目10番３号
(74)代理人　弁理士　佐藤　辰彦　（外１名）

(54)【発明の名称】　電子契約方法

(57)【要約】
【課題】契約の当事者間で、共通の鍵を使用した暗号通信を行いつつ契約の信頼性を高めることができると共に、簡易で普及性の高い電子契約システムを構築することができる電子契約方法を提供する。
【解決手段】ユーザーＢがユーザーＡから契約の締結の意思表示を受けたとき、ユーザーＢは自身の端末装置によって一回性の数を種とする乱数を生成し、それをユーザーＡとの共通鍵K_{AB}で暗号化してユーザーＡに送信する。ユーザーＡは乱数を共通鍵K_{AB}で復号化し、その乱数を鍵として契約内容を暗号化してユーザーＢに送信し、ユーザーＢに契約を申し込む。さらにユーザーＡは契約内容を自身の秘密鍵K_{SA}により定まるハッシュ関数で変換して成る認証データをユーザーＢに送信する。

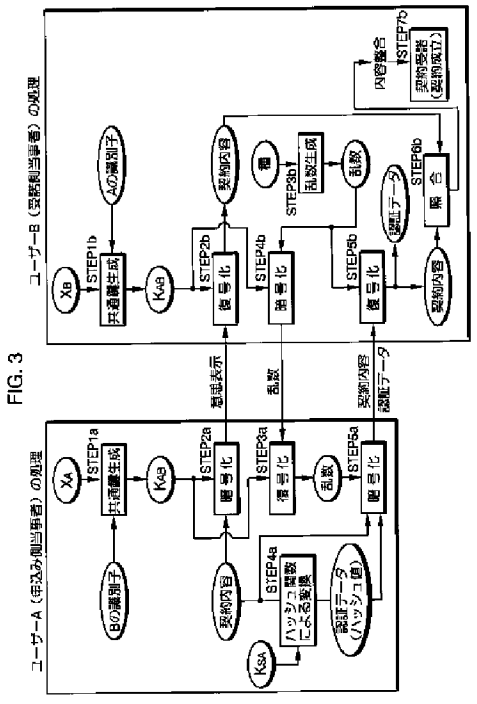


FIG. 3

1

【特許請求の範囲】

【請求項１】ネットワーク上の二人の当事者の一方を契約の申込み側、他方を該契約の受諾側として、両当事者がそれぞれ所持する端末装置間のオンライン通信により前記契約を行う電子契約方法において、

各当事者の端末装置に、あらかじめ前記契約を行う相手側の当事者の識別子を入力することにより両当事者間でのみ有効な暗号通信用の共通鍵を生成する手段と、通信データの暗号・復号化を行う手段とを具備しておき、

前記受諾側当事者は、前記申込み側当事者から前記契約の締結の意思表示を受けたとき、該受諾側当事者の端末装置により、前記申込み側当事者の識別子を入力して該申込み側当事者との前記共通鍵を生成した後、前記申込み側当事者には不知で該受諾側当事者に固有の受諾側固有データを前記共通鍵を用いて暗号化して前記申込み側当事者の端末装置に送信し、

その暗号化された前記受諾側固有データを受信した前記申込み側当事者は、該申込み側当事者の端末装置により、前記受諾側当事者の識別子を入力して該受諾側当事者との前記共通鍵を生成した後、その共通鍵を用いて前記暗号化された受諾側固有データを復号化し、さらに、前記受諾側当事者と契約しようとする契約内容を、前記復号化した受諾側固有データを鍵として用いて暗号化した後、その暗号化した契約内容を前記受諾側当事者の端末装置に送信することにより前記受諾側当事者に前記契約を申込み、

前記受諾側固有データを鍵として暗号化された前記契約内容を受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記暗号化された契約内容を該受諾側当事者の前記受諾側固有データを鍵として用いて復号化し、その復号化した前記契約内容に基づき、前記契約を受諾することを特徴とする電子契約方法。

【請求項２】前記受諾側当事者は、前記受諾側固有データを暗号化して前記申込み側当事者に送信する前に、該受諾側当事者の端末装置により、一回性の数を種として該種が逆算不能な乱数を生成し、その生成した乱数を前記受諾側固有データとして用いることを特徴とする請求項１記載の電子契約方法。

【請求項３】前記乱数の種となる前記一回性の数は、前記受諾側当事者の端末装置における人為的入力操作の時間的タイミングに基づき生成することを特徴とする請求項２記載の電子契約方法。

【請求項４】前記申込み側当事者は、前記受諾側当事者に前記契約の締結の意思表示をするとき、前記契約内容又はその概要を示す予備契約内容を、前記受諾側当事者との前記共通鍵を用いて該申込み側当事者の端末装置により暗号化して前記受諾側当事者の端末装置に送信し、

前記受諾側当事者は、前記契約を受諾する際に、前記共通鍵を用いて暗号化された前記契約内容又は予備契約内容を該受諾側当事者の端末装置により復号化したもの

2

と、前記受諾側固有データを鍵として暗号化された前記契約内容を該受諾側当事者の端末装置により復号化したものとを照合して、該契約内容を確認することを特徴とする請求項１乃至３のいずれかに記載の電子契約方法。

【請求項５】前記申込み側は、前記契約を前記受諾側当事者に申し込む際に、該申込み側当事者の端末装置により、少なくとも前記契約内容に、該申込み側当事者及び前記受諾側当事者以外の公証能力を有する第三者が認証可能な該申込み側当事者に固有の秘密鍵に基づく加工を施して該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、その生成した認証データを前記受諾側当事者に送信することを特徴とする請求項１乃至４のいずれかに記載の電子契約方法。

【請求項６】前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、前記秘密鍵により定まる一方向性関数により変換することにより生成することを特徴とする請求項５記載の電子契約方法。

【請求項７】前記契約の申込みの日時に応じたデータは、該日時を示す数値を前記一方向性関数又は該一方向性関数とは異なる一方向性関数により変換してなるデータであることを特徴とする請求項６記載の電子契約方法。

【請求項８】前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、所定の一方向性関数により変換した後、その変換データを前記秘密鍵により暗号化することにより生成することを特徴とする請求項５記載の電子契約方法。

【請求項９】前記契約の申込みの日時に応じたデータは、該日時を示す数値を前記一方向性関数又は該一方向性関数とは異なる一方向性関数により変換してなるデータであることを特徴とする請求項８記載の電子契約方法。

【請求項１０】前記申込み側当事者は、前記契約を前記受諾側当事者に申し込む際に、前記一方向性関数により得られた前記変換データを前記受諾側当事者の端末装置に送信し、

該変換データを受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記受諾側固有データを鍵として復号化した前記契約内容を、前記申込み側当事者の一方向性関数と同一の一方向性関数により変換し、さらに、前記契約を受諾する際に、前記受諾側当事者の端末装置から送信されてきた前記変換データと、前記受諾側固有データを鍵として復号化した前記契約内容を前記申込み側当事者の一方向性関数と同一の一方向性関数により変換してなるデータとを照合して前記変換データを確

認することを特徴とする請求項８又は９記載の電子契約方法。

【請求項１１】前記申込み側当事者は、前記変換データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された変換データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することを特徴とする請求項１０記載の電子契約方法。

【請求項１２】前記申込み側当事者は、前記認証データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された認証データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することを特徴とする請求項５乃至１１のいずれかに記載の電子契約方法。

【請求項１３】前記契約の締結後に、前記申込み側当事者及び受諾側当事者は、少なくとも前記契約内容と前記受諾側固有データと前記変換データと前記認証データとを前記第三者に送って保管せしめることを特徴とする請求項１０乃至１２のいずれかに記載の電子契約方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット、パソコン通信網等のネットワークを用いたオンライン通信によって、商品の売買やそれに伴う課金、決済等を含む、各種の契約を行う電子契約方法に関する。

【０００２】

【従来の技術】ネットワーク上の二人の当事者間で、その一方を契約の申込み側、他方を契約の受諾側としてオンライン通信によって各種の契約を結ぶ場合、その契約を安全に行い、該契約の信頼性を高めるためには、契約内容を第３者が偽造できない（Third party condition。以下、条件Ｔという）、契約内容を受信者（契約の受諾者）が偽造できない（Reciever condition。以下、条件Ｒという）、契約内容を送信者（契約の申込み者）が事後否定できない（Sender condition。以下、条件Ｓという）というような条件が満たされることが必要であると一般に言われている（例えばW.Diffie及びM.E.Hellman による論文「New directions in cryptography／IEEE, IT, vol.IT-22,No.6, pp.644-654, 1976.11.」を参照）。特に、商品の売買契約等においては、前記条件Ｓが不充分であると、後々の当事者間の争いの元となることが多く、この条件Ｓを可能な限り満たすことが望ましい。

【０００３】ところで、従来の電子契約の手法としては、例えば契約の申込み者に固有のパスワードを利用したものが一般に普及している。

【０００４】この手法では、例えばネットワーク上の契約の申込み側当事者としてのあるユーザが、契約の受諾側当事者としての商品販売者から商品を購入する契約を結ぼうとするとき、該ユーザはあらかじめ商品販売者に登録した該ユーザの固有のパスワードを使用して該商品販売者に商品購入の申込みをオンライン通信で行う。そして、その申込みの通信を受けた商品販売者は、上記パスワードに基づきユーザを認証して、該ユーザによる商品購入やその代金支払いの申込みを受諾し、その受諾した内容に従って商品をユーザに受け渡したり、代金請求を行ったりする。

【０００５】しかるに、この手法では、ユーザと商品販売者との間で契約内容やパスワードがそのまま通信されるため、パスワードが第三者に盗用されたり、契約内容が第三者により偽造されたりする危険性が高い。このため、例えば前記条件Ｔを満たすことが難しく、信頼性の高い契約を行うことが困難である。

【０００６】また、近年では、所謂、ＲＳＡ暗号を用いた公開鍵方式による電子契約の手法も知られている。

【０００７】この手法では、例えば前記のような商品購入の契約を行うとき、ユーザは、商品購入の申込み内容を、ネットワーク上の鍵管理局から与えられた該ユーザに固有の秘密鍵を用いて暗号化し、それを商品販売者に送信する。また、その暗号化された申込みを受けた商品販売者側では、鍵管理局が公開しているユーザの公開鍵を参照し、その公開鍵を用いて暗号化された申込み内容を復号化する。そして、この復号化した申込み内容に基づき、ユーザによる商品購入やその代金支払いの申込みを受諾する。この場合、ユーザの公開鍵を用いて正常に復号化することができるのは、該ユーザの秘密鍵を用いて暗号化されたものだけであるので、商品販売者はユーザから受けた申込み内容が正常に復号化されるか否かによって、ユーザを認証することができる。

【０００８】このような公開鍵方式による手法では、契約の当事者間の通信は暗号によって行われるため、その通信内容の機密性が確保され、第三者による契約内容の偽造等が困難である。また、契約の申込み側当事者であるユーザの公開鍵によって復号化できる暗号文は該ユーザの秘密鍵によって暗号化されたものに限るため、ユーザが契約事実を事後否定したり、契約の受諾側当事者である商品販売者が契約内容を偽造することも困難となる。従って、前記条件Ｔ，Ｒ，Ｓを満たし易く、契約の信頼性を高めることができる。

【０００９】しかるに、この公開鍵方式では、一般にその暗号通信のためのデータ処理量が大きなものとなって非効率なものとなり易く、また、通信に際して、その都度、公開鍵の参照等のために鍵管理局と通信を行ったりしなければならず、手間のかかるものとなっていた。さらに、鍵管理局では、公開鍵を厳格に保守・管理しなければならないため、該鍵管理局の負担が大きく、多数のユーザがシステムに加入することが困難である。従って、このような公開鍵方式による手法では、簡易で普及

性の高い電子契約システムを構築することが困難なものとなっていた。

【００１０】一方、暗号通信においては、前記公開鍵方式のように暗号化と復号化とで異なる鍵を使用する非対称型の暗号通信方式の他、暗号化と復号化とで同じ鍵を使用する対称型の暗号通信方式が知られている。そして、このような対称型の暗号通信方式としては、例えばRolf Blomによる論文「NON-PUBLIC KEY DISTRIBUTION／Advances in Cryptology:Proceedings of CRYPTO '82／Plenum Press 1983,pp.231-236」、同じくRolf Blomによる論文「An Optimal Class of SymmetricKey Generation Systems／Advances in Cryptology: EUROCRYPT '84／Springer LNCS 209, 1985,pp.335-338」、あるいは特公平５－４８９８０号公報もしくは米国特許第５０１６２７６号に見られるように、あらかじめ鍵管理局から各ユーザに、該ユーザ固有の個人鍵（アルゴリズム）を配付しておき、通信に際しては、各ユーザが自己の個人鍵に通信相手側の名前等の公開性の識別子を入力することで、その通信相手側との暗号通信を行うための共通鍵を生成することができるようにしたものが知られている。

【００１１】このような暗号通信方式によれば、各ユーザは、暗号通信を行う際には、鍵管理局との事前通信等を行うことなく、自己の個人鍵に通信相手側の名前等の公開性の識別子を入力するだけで、随時、通信相手側との暗号通信用の共通鍵を生成することができ、また、鍵管理局は、各ユーザの個人鍵を発行すればよいだけなので、その負担も小さい。

【００１２】従って、このような共通鍵による暗号通信方式を電子契約に適用できれば、簡易で普及性の高い電子契約システムを提供することができると考えられる。

【００１３】しかしながら、このような共通鍵による暗号通信方式を用いてオンライン通信による契約を行おうとした場合、その契約の両当事者が、いつでも随意に、相手側との共通鍵を生成できるため、単に、契約内容を共通鍵により暗号化して両当事者間で授受しただけでは、契約の信頼性を充分に確保することが困難である。

【００１４】すなわち、二者間で契約を締結する場合、その契約の信頼性を高める上で、前記条件Ｔ，Ｒ，Ｓが満たされることも一つの要件として重要ではあるが、その他に、書面による通常的な契約の場合における各当事者の署名や捺印等、各当事者にしかなしえず、より好ましくは、当事者以外の者が公的に認証し得るものを相手側の当事者に与えることが重要である。しかるに、前述のように、共通鍵を用いた暗号通信により契約を結ぼうとした場合、該共通鍵は、両当事者が随時生成することができるものであるため、単に、契約内容を共通鍵により暗号化して両当事者間で授受しただけでは、各当事者は互いに相手側に各当事者しかなし得ないものを与えることができず、契約の信頼性を充分に確保することが困難である。

【００１５】

【発明が解決しようとする課題】本発明はかかる背景に鑑み、契約の当事者間で、共通の鍵を使用した暗号通信を行いつつ契約の信頼性を高めることができると共に、簡易で普及性の高い電子契約システムを構築することができる電子契約方法を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の電子契約システムははかかる目的を達成するために、ネットワーク上の二人の当事者の一方を契約の申込み側、他方を該契約の受諾側として、両当事者がそれぞれ所持する端末装置間のオンライン通信により前記契約を行う電子契約方法において、各当事者の端末装置に、あらかじめ前記契約を行う相手側の当事者の識別子を入力することにより両当事者間でのみ有効な暗号通信用の共通鍵を生成する手段と、通信データの暗号・復号化を行う手段とを具備しておき、前記受諾側当事者は、前記申込み側当事者から前記契約の締結の意思表示を受けたとき、該受諾側当事者の端末装置により、前記申込み側当事者の識別子を入力して該申込み側当事者との前記共通鍵を生成した後、前記申込み側当事者には不知で該受諾側当事者に固有の受諾側固有データを前記共通鍵を用いて暗号化して前記申込み側当事者の端末装置に送信し、その暗号化された前記受諾側固有データを受信した前記申込み側当事者は、該申込み側当事者の端末装置により、前記受諾側当事者の識別子を入力して該受諾側当事者との前記共通鍵を生成した後、その共通鍵を用いて前記暗号化された受諾側固有データを復号化し、さらに、前記受諾側当事者と契約しようとする契約内容を、前記復号化した受諾側固有データを鍵として用いて暗号化した後、その暗号化した契約内容を前記受諾側当事者の端末装置に送信することにより前記受諾側当事者に前記契約を申込み、前記受諾側固有データを鍵として暗号化された前記契約内容を受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記暗号化された契約内容を該受諾側当事者の前記受諾側固有データを鍵として用いて復号化し、その復号化した前記契約内容に基づき、前記契約を受諾することを特徴とする。

【００１７】かかる本発明によれば、前記受諾側当事者は、前記申込み側当事者から契約の締結の申込みを受けたとき、該受諾側当事者に固有で且つ申込み側当事者には不知の前記受諾側固有データを、申込み側当事者との前記共通鍵を用いて暗号化して、申込み側当事者の端末装置に送信する。この場合、申込み側当事者との共通鍵は、受諾側当事者の端末装置に該受諾側当事者の通信相手である申込み側当事者の識別子を入力することで生成される。

【００１８】一方、上記のように暗号化された前記受諾側固有データを自身の端末装置で受信した前記申込み側

当事者は、その暗号化された受諾側固有データを受諾側当事者との前記共通鍵を用いて復号化する。この場合、受諾側当事者との共通鍵は、申込み側当事者の端末装置に受諾側当事者の氏名等の識別子を入力することで生成される。

【００１９】尚、各当事者が前述の如く通信相手側との共通鍵を生成するために必要な各当事者の識別子は、各当事者の氏名、住所、ネットワーク上のメールアドレス、ドメイン名、あるいはそれらを組み合わせたもの等、各当事者に固有で且つ公開性のあるものを使用する。

【００２０】次に、上記のように受諾側固有データを復号化した申込み側当事者は、その受諾側固有データを鍵として、前記契約内容を暗号化して受諾側当事者の端末装置に送信し、これにより前記契約を受諾側当事者に申し込む。そして、このように受諾側固有データを鍵として暗号化された前記契約内容を自身の端末装置で受信した受諾側当事者は、自身が所持する前記受諾側固有データを鍵として、該契約内容を復号化し、その復号化した契約内容に基づき申込み側当事者との契約を受諾する。

【００２１】このような契約を行う本発明の電子契約方法によれば、申込み側当事者は、受諾側当事者に固有で、しかも該申し込み側当事者が事前には知り得ない受諾側固有データを鍵として契約内容を暗号化して、受諾側当事者に契約を申し込むので、受諾側当事者は、自身が独自に指定した独特な方式で申込み側当事者からの契約の申込みを受けることとなる。このため、該受諾側当事者にとっては、申込み側当事者による契約の申込みの信頼性が高まる。同時に、申込み側当事者は、受諾側当事者が独自に指定した方式に従って契約を申し込むこととなるため、契約の事後否定をしにくくなる。また、受諾側当事者から申込み側当事者への前記受諾側固有データの暗号通信のための前記共通鍵は、両当事者がそれぞれ各別に自身の端末装置に相手側の識別子を入力するだけで両当事者が共有することができ、さらに、申込み側当事者から受諾側当事者への前記契約内容の暗号通信のための鍵は、その鍵としての前記受諾側固有データを受諾側当事者から申込み側当事者に前記共通鍵により暗号化して与えるだけで、両当事者が共有することができるので、鍵管理局等の第三者の関与を伴うことなく、両当事者だけで、支障なく契約のための通信を行うことができる。さらには、両当事者間の通信は暗号通信によって行われるので、その通信データ（受諾側固有データ及び契約内容）の部外者に対する機密性が保たれる。

【００２２】従って、本発明によれば、契約の当事者間で、共通の鍵を使用した暗号通信を行いつつ契約の信頼性を高めることができると共に、簡易で普及性の高い電子契約システムを構築することができる。

【００２３】かかる本発明では、前記受諾側当事者は、前記受諾側固有データを暗号化して前記申込み側当事者に送信する前に、該受諾側当事者の端末装置により、一回性の数を種として該種が逆算不能な乱数を生成し、その生成した乱数を前記受諾側固有データとして用いることが好ましい。ここで、前記一回性の数は、再現性がなく、もしくは再現性に極めて乏しい数である。

【００２４】このように受諾側当事者の端末装置で一回性の数を種として生成した乱数を前記受諾側固有データとして用いることで、受諾側当事者における該受諾側固有データの独自色が強まり、このような受諾側固有データを鍵として、前記申込み側当事者から前記契約内容を暗号化して受諾側当事者に送信することで、その契約内容に基づく、両当事者間の契約の信頼性が効果的に高まる。

【００２５】この場合、前記乱数の種となる前記一回性の数は、例えば前記受諾側当事者の端末装置における人為的入力操作の時間的タイミングに基づき生成する。このように、受諾側当事者の端末装置における人為的入力操作（例えばある文章や語句を入力する操作）の時間的タイミングに基づき生成される数は、人間による操作のあいまいさによって、偶然的で予想のつかないものとなる。従って、再現性がなく、もしくは再現性に極めて乏しい一回性の数を的確に生成することができ、その数を種として生成した乱数を受諾側固有データとして使用することで、該受諾側固有データの独自性を良好に確保することができる。

【００２６】また、本発明では、前記申込み側当事者は、前記受諾側当事者に前記契約の締結の意思表示をするとき、前記契約内容又はその概要を示す予備契約内容を、前記受諾側当事者との前記共通鍵を用いて該申込み側当事者の端末装置により暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、前記契約を受諾する際に、前記共通鍵を用いて暗号化された前記契約内容又は予備契約内容を該受諾側当事者の端末装置により復号化したものと、前記受諾側固有データを鍵として暗号化された前記契約内容を該受諾側当事者の端末装置により復号化したものとを照合して、該契約内容を確認する。

【００２７】このように、申込み側当事者が、受諾側当事者に契約の締結の意思表示を行う際に、前記共通鍵を用いた暗号通信によって、前記契約内容又はその概要を示す予備契約内容を受諾側当事者に与えておくことで、受諾側当事者は、最終的に契約を承諾するに際して、前記共通鍵を用いて暗号化された前記契約内容又は予備契約内容を復号化したものと、前記受諾側固有データを鍵として暗号化された前記契約内容を復号化したものとを照合して、それらの整合性を確認した上で、契約を承諾することができ、該受諾側当事者にとって、申込み側当事者との契約の信頼性をより一層高めることができる。

【００２８】さらに、本発明では、前記申込み側は、前記契約を前記受諾側当事者に申し込む際に、該申込み側

当事者の端末装置により、少なくとも前記契約内容に、該申込み側当事者及び前記受諾側当事者以外の公証能力を有する第三者が認証可能な該申込み側当事者に固有の秘密鍵に基づく加工を施して該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、その生成した認証データを前記受諾側当事者に送信する。

【００２９】このように、前記申込み側当事者が受諾側当時者に契約を申し込む際に、前記契約内容に、前記申込み側当事者に固有でしかも前記第三者が認証可能な秘密鍵に基づく加工を施して、該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、それを受諾側当事者に送信することで、受諾側当事者には、前記契約内容に申込み側当事者が公的な署名もしくは捺印を施したものに相当する認証データが申込み側当事者から与えられることとなる。これにより、両当事者にとって、契約の信頼性がより強固なものとなる。

【００３０】この場合、前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、前記秘密鍵により定まる一方向性関数により変換する。

【００３１】あるいは、前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、所定の一方向性関数により変換した後、その変換データを前記秘密鍵により暗号化することにより生成する。

【００３２】これによれば、前記契約内容もしくはこれを前記受諾側固有データを鍵として暗号化したもの、又はこれらに契約の日時を応じたデータを付加したもの（以下、ここでは契約内容等と称する）と申込み側当事者とに固有の認証データを的確に生成することができる。また、認証データの生成に際して、契約内容等を一方向性関数を用いて変換するので、生成した認証データを受諾側当事者に与えた後に、例えば申込み側当事者が契約内容を改ざんしようとしても、該申込み側当事者は、受諾側当事者に与えた認証データと整合するように契約内容を改ざんすることは難しく、申込み側当事者が契約内容を事後否定することは困難なものとなる。また、前記認証データは、申込み側当事者の秘密鍵に基づいて生成されるので、例えば該申込み側当事者が、受け取った認証データに整合するように契約内容を改ざんすることも困難である。従って、前記契約の信頼性を両当事者間で効果的に高めることができる。

【００３３】尚、前記契約の申込みの日時に応じたデータを付加する場合、前記契約の申込みの日時に応じたデータは、該日時を示す数値を前記一方向性関数又は該一方向性関数とは異なる一方向性関数により変換してなるデータであることが好ましい。このように契約の日時を一方向性関数により変換しておくことで、後に、契約の申込みの日時を改ざんしよとしても、その改ざんが困難なものとなる。

【００３４】前述のように前記契約内容等を所定の一方向性関数により変換した後、その変換データを前記秘密鍵を鍵として暗号化する場合、前記申込み側当事者は、前記契約を前記受諾側当事者に申し込む際に、前記一方向性関数により得られた前記変換データを前記受諾側当事者の端末装置に送信し、該変換データを受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記受諾側固有データを鍵として復号化した前記契約内容を、前記申込み側当事者の一方向性関数と同一の一方向性関数により変換し、さらに、前記契約を受諾する際に、前記受諾側当事者の端末装置から送信されてきた前記変換データと、前記受諾側固有データを鍵として復号化した前記契約内容を前記申込み側当事者の一方向性関数と同一の一方向性関数により変換してなるデータとを照合して前記変換データを確認することが好ましい。

【００３５】このように前記契約内容等を申込み側当事者が所定の一方向性関数により変換して成る変換データを受諾側当事者に送信し、また、受諾側当事者にあっては、前記受諾側固有データを鍵として復号化した前記契約内容を申込み側当事者と同じ一方向性関数によって変換してなるデータと、前記受諾側当事者から送られてきた変換データとを照合することで、前記変換データが正式な契約内容（受諾側固有データを鍵として復号化した契約内容）に基づいて生成されたものであるか否かを確認することができる。これにより、契約の信頼性をさらに高めることができる。

【００３６】尚、前記変換データの通信においては、前記申込み側当事者は、前記変換データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された変換データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することが好ましい。

【００３７】また、前記認証データの通信においては、前記申込み側当事者は、前記認証データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された認証データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することが好ましい。

【００３８】このように契約の信頼性を高める上で重要な前記変換データや認証データを暗号化して通信することで、該変換データや認証データの部外者に対する機密性を確実に確保することができる。

【００３９】また、契約に際して、前記認証データや変換データを通信する場合、前記契約の締結後に、前記申

込み側当事者及び受諾側当事者は、少なくとも前記契約内容と前記受諾側固有データと前記変換データと前記認証データとを前記第三者に送って保管せしめることが特に好適である。

【００４０】このように、各当事者が前記契約内容や前記受諾側固有データ、前記変換データ、前記認証データをこれらの当事者から中立的な第三者に送って保管せしめることで、契約の効力を確実なものとすることができる。

【００４１】

【発明の実施の形態】本発明の第１の実施形態を図１乃至図３を参照して説明する。図１は本実施形態の電子契約方法を適用した電子契約システムの全体的構成を示す説明図、図２は本実施形態において契約を行う当事者が所持する端末装置の機能的構成を示すブロック図、図３は本実施形態で契約を行う際の処理手順を示すフロー図である。

【００４２】図１を参照して、本システムでは、複数のユーザーＡ，Ｂ，…がそれぞれ所持する端末装置１ａ，１ｂ，…と、暗号通信用の鍵の発行等を担う鍵管理局Ｃの端末装置２と、暗号通信用の鍵の認証等を行う公証人Ｓの端末装置３とがインターネット、パソコン通信網等のネットワーク４を介して相互に通信可能に接続されている。各端末装置１ａ，１ｂ，…，２，３は、パソコン等のコンピュータマシンや通信機器、あるいはそれらに付帯したソフトウェア等により構成されている。　この場合、各ユーザーＡ，Ｂ，…には、他の任意のユーザーとの間での暗号通信用の共通鍵を生成するための各ユーザーＡ，Ｂ，…に固有の共通鍵生成用アルゴリズムX_A，X_B，…があらかじめ鍵管理局Ｃから配付されると共に、公証人Ｓとの間での暗号通信用の共通鍵K_{AS}，K_{BS}，…が各ユーザーＡ，Ｂ，…に固有の秘密鍵としてあらかじめ鍵管理局Ｃから配付されている。それらの共通鍵生成用アルゴリズムX_A，X_B，…や秘密鍵K_{AS}，K_{BS}，…は、それぞれ各ユーザーＡ，Ｂ，…の端末装置１ａ，１ｂ，…（以下、必要に応じて端末装置１と総称する）に保管されている。

【００４３】また、前記公証人Ｓには、任意のユーザーＡ，Ｂ，…との間での暗号通信用の共通鍵K_{AS}，K_{BS}，…（＝各ユーザーＡ，Ｂ，…の秘密鍵）を生成するための該公証人Ｓに固有の共通鍵生成用アルゴリズムX_Sがあらかじめ鍵管理局Ｃから配付され、それが公証人Ｓの端末装置３に保管されている。これにより、公証人Ｓは、必要に応じて、自身の共通鍵生成用アルゴリズムX_Sを用いて、各ユーザーＡ，Ｂ，…との共通鍵K_{AS}，K_{BS}，…を生成し、それを各ユーザーＡ，Ｂ，…が所持する秘密鍵K_{AS}，K_{BS}，…と照合することで、各ユーザーＡ，Ｂ，…の秘密鍵K_{AS}，K_{BS}，…を認証することができるようになっている。

【００４４】ここで、各ユーザーＡ，Ｂ，…や公証人Ｓが所持する共通鍵生成用アルゴリムムX_A，X_B，…，X_Sは、前述のRolf Blom の論文や特公平５－４８９８０号公報、米国特許第５０１６２７６号に見られるもののように、通信相手側の名前、住所等、その通信相手に固有で公開性のある識別子を入力することでその通信相手側との暗号通信用の共通鍵を生成するものである。

【００４５】図２に示すように、各ユーザーＡ，Ｂ，…の端末装置１には、そのハードウェアやソフトウェアによる機能的構成として、乱数を生成する乱数生成手段５と、前述の如く通信相手側の識別子を入力することで前記共通鍵生成用アルゴリズムX_A，X_B，…により、その通信相手側との暗号通信用の共通鍵を生成する共通鍵生成手段６と、該共通鍵生成手段６により生成される共通鍵や前記乱数生成手段５により生成される乱数を鍵として、所謂、鍵共有方式による通信データの暗号化・復号化を行う暗号・復号手段７と、通信データの送信及び受信を行う通信手段８と、後述の契約のための各種データの生成等の処理を担う契約処理システム９（詳細は後述する）とが備えられている。

【００４６】この場合、暗号・復号手段７は、例えば３段のＤＥＳ（Data Encryption Standard）により構成され、通信手段８は、モデムや通信処理用のソフトウェアにより構成されている。

【００４７】また、乱数生成手段５は、一回性の数を種として、前記暗号・復号手段７に対する鍵として使用可能な乱数を生成するものである。具体的には、該乱数生成手段５により乱数を生成するに際しては、例えば端末装置１のユーザーにより、ある語句もしくは文章等が図示しないキーボードから端末装置１に入力され、このとき、乱数生成手段５は、その入力操作のタイミング（例えば各単語の入力時刻や各単語の入力の時間間隔）を計測する。この入力操作のタイミングの計測値は、あいまいさを有する人為的な入力操作に基づくため、偶然的で再現性のない一回性の数に相当するものとなる。そして、乱数生成手段５は、その入力操作のタイミングの計測値を種として、該計測値を前記暗号・復号手段７の暗号化・復号化のための鍵として使用可能なデータに変換することで、乱数を生成する。この場合、前記計測値を乱数に変換するに際しては、例えばハッシュ関数等の一方向性関数による変換を行うことで、その変換結果として得られた乱数からその種である前記計測値を逆算することができないものとされる。このようにして乱数生成手段５により生成する乱数は、各ユーザーＡ，Ｂ，…同士の後述の契約に際して、その契約の受諾側当事者となるユーザー側の端末装置１において、該受諾側当事者に固有で、契約の申込み側当事者には予想のつかない受諾側固有データとして生成されるものである。

【００４８】以上のような構成を有する本実施形態のシステムでは、例えばユーザーＡがユーザーＢから商品を購入したり、サービスの提供を受けるための契約等、ユ

ーザーＡを契約の申込み側当事者、ユーザーＢを契約の受諾側当事者とした契約を両者間で締結する場合に、その契約は次のようにして行われる。

【００４９】すなわち、図３を参照して、まず、契約の申込み側当事者であるユーザーＡは、自身の端末装置１ａにおいて、契約の受諾側当事者であるユーザーＢの識別子を入力し、そのユーザーＢの識別子と前記共通鍵生成用アルゴリズムX_Aとから前記共通鍵生成手段６により、ユーザーＢとの共通鍵K_{AB}を生成する（ＳＴＥＰ１ａ）。

【００５０】次いで、ユーザーＢと締結しようとする契約内容（これはユーザーＡが端末装置１ａ上で別途作成しておく）を、端末装置１ａの暗号・復号手段７により、ＳＴＥＰ１ａで生成した共通鍵K_{AB}を用いて暗号化し、その暗号化した契約内容を通信手段８を介してユーザーＢの端末装置１ｂに送信する（ＳＴＥＰ２ａ）。これにより、ユーザーＡは、ユーザーＢに対して、契約の締結の意思表示を行う。

【００５１】尚、この意思表示のために暗号化して送信する内容は、ユーザーＡが最終的にユーザーＢと締結しようとする契約内容そのものでなくてもよく、該契約内容の概要（骨子）を表した予備的な内容のものであってもよい。

【００５２】一方、上記の送信を受けたユーザーＢは、自身の端末装置１ｂにおいて、ユーザーＡの識別子を入力し、そのユーザーＡの識別子と前記共通鍵生成用アルゴリズムX_Bとから前記共通鍵生成手段６により、ユーザーＡとの共通鍵K_{AB}を生成する（ＳＴＥＰ１ｂ）。

【００５３】次いで、ユーザーＢは、前記乱数生成手段５によって、前述の如く該ユーザーＢの端末装置１ｂへの入力操作のタイミングに基づく一回性の数（入力操作のタイミングの計測値）を種とした乱数を受諾側固有データとして生成する（ＳＴＥＰ２ｂ）。

【００５４】そして、ユーザーＢは、端末装置１ｂの暗号・復号手段７により、ＳＴＥＰ２ｂで生成した乱数を、ＳＴＥＰ１ｂで生成した共通鍵K_{AB}を用いて暗号化し、その暗号化した乱数を通信手段８を介してユーザーＡの端末装置１ａに送信する（ＳＴＥＰ３ｂ）。

【００５５】この暗号化された乱数を受信したユーザーＡは、その暗号化された乱数を、自身の端末装置１ａの暗号・復号手段７によって、前記ＳＴＥＰ１ａで生成した共通鍵K_{AB}を用いて復号化する（ＳＴＥＰ３ａ）。

【００５６】また、ユーザーＡは、自身の端末装置１ａの前記契約処理システム９により、ユーザーＢと締結しようとする契約内容と該ユーザーＡとに固有の認証データを生成する（ＳＴＥＰ４ａ）。すなわち、契約処理システム９は、ユーザーＡの前記秘密鍵K_{SA}をパラメターとして決定される一方向性関数としてのハッシュ関数を有しており、認証データの生成指示がユーザーＡから与えられたとき、このハッシュ関数により契約内容を変換することで、認証データ（ハッシュ値）を生成する。このように生成される認証データは、契約内容を、ユーザーＡの秘密鍵K_{SA}により定まるハッシュ関数によって変換したものであるため、契約内容とユーザーＡとに固有のものとなる。

【００５７】次いで、ユーザーＡは、このようにして生成した認証データとその元文である契約内容とを一括したものを、端末装置１ａの暗号・復号手段７によって、前記ＳＴＥＰ３ａで復号した乱数（受諾側固有データ）を鍵として暗号化し、その暗号化した認証データ及び契約内容をユーザーＢの端末装置１ｂに送信する（ＳＴＥＰ５ａ）。これによりユーザーＡはユーザーＢに契約を申し込む。

【００５８】上記のように暗号化された認証データ及び契約内容を受信したユーザーＢは、その暗号化された認証データ及び契約内容を、端末装置１ｂの暗号・復号手段７によって、前記ＳＴＥＰ３ｂで生成した乱数を鍵として復号化することで、暗号化されていない本来の認証データ及び契約内容を取得する（ＳＴＥＰ５ｂ）。さらに、ユーザーＢはＳＴＥＰ５ｂで取得した契約内容と、前記ＳＴＥＰ２ｂで取得した契約内容とを照合し（ＳＴＥＰ６ｂ）、それらの内容の整合を確認した上で、ユーザーＡから前述の如く申し込まれた契約を受諾し（ＳＴＥＰ７ｂ）、これによりユーザーＡ，Ｂ間の契約が成立する。

【００５９】尚、ユーザーＡは、前記ＳＴＥＰ３ａで復号化した乱数や、ＳＴＥＰ５ａで暗号化する前の認証データ及び契約内容を保管しておき、ユーザーＢは、ＳＴＥＰ３ｂで生成した乱数もしくはこの乱数の種とした一回性の数や、ＳＴＥＰ５ｂで復号化した認証データ及び契約内容を保管しておく。このような本実施形態の電子契約によれば、ユーザーＢは、ユーザーＡから契約の意思表示を受けたとき、ユーザーＢに固有で、しかもユーザーＡには判らない一回性の数を種として生成した乱数をユーザーＡに与え、この乱数を鍵として暗号化された契約内容をユーザーＡから受け取るため、ユーザーＢは、自身が独自にユーザーＡに対して指定した該ユーザーＢに固有の方式で、ユーザーＡから前記契約内容に従った契約の申込みを受けることとなる。

【００６０】このため、ユーザーＢにとっては、ユーザーＡによる契約の締結の意思が明確なものとなる。同時に、ユーザーＡはユーザーＢにより指定された独特の方式でユーザーＢに契約を申し込むこととなるため、契約事実を事後否定しにくくなる。従って、ユーザーＢにとって、ユーザーＡから申し込まれた契約の信頼性が高まる。

【００６１】さらに、ユーザーＡは、ユーザーＢに最初に契約の締結の意思表示をするに際して、ユーザーＢと締結しようとする契約内容あるいはその概要（骨子）をユーザーＢに与えておくため、ユーザーＢは、最終的に

15

ユーザーＡとの契約を受諾するに際して、最初に受け取った契約内容もしくはその概要（ＳＴＥＰ２ｂで復号化したもの）と、最終的に受け取った契約内容（ＳＴＥＰ５ｂで復号化したもの）とを照合して両者の矛盾の有無を確認した上で、ユーザーＡとの契約を受諾することができ、これによっても、ユーザーＡとの契約の信頼性が高まる。

【００６２】また、ユーザーＡは、自身に固有の秘密鍵K_{SA}によって定まるハッシュ関数（一方向性関数）によって、契約内容を変換してなる認証データをユーザーＢに与えるため、ユーザーＡ，Ｂの両者にとっての契約の信頼性が一層強固なものとなる。

【００６３】すなわち、前記認証データは、ユーザーＡに固有の秘密鍵K_{SA}によって定まるハッシュ関数（一方向性関数）によって、契約内容を変換したものであるため、ユーザーＡと契約内容とに固有で、しかも、ユーザーＢには生成することができないものである。そして、ユーザーＡの秘密鍵K_{SA}は、ユーザーＡ，Ｂの両者から中立的な立場にある前記公証人Ｓが必要に応じて認証可能なものである。このため、前記認証データをユーザーＡからユーザーＢに与えるということは、ユーザーＡが、ユーザーＢと締結する契約内容に公的な署名もしくは捺印を施したものをユーザーＢに与えるということを意味する。

【００６４】この場合、ユーザーＢは、ユーザーＡから認証データを受け取った時点では、その認証データが適正なものであるか否かは判らないものの、必要に応じて公証人Ｓによって、ユーザーＢあるいはユーザーＡが保管している契約内容をユーザーＡの秘密鍵K_{SA}により定まるハッシュ関数で変換してもらい、それをユーザーＡからユーザーＢに与えられた認証データと照合することで、ユーザーＡからユーザーＢに与えられた認証データの真偽を証明してもらうことができる。

【００６５】また、ユーザーＢは、認証データに反映されるユーザーＡの秘密鍵K_{SA}を知らないため、仮にユーザＢがユーザーＡとの契約の締結後に、ユーザーＡから受け取った契約内容を改ざんしようとしても、その改ざんした契約内容と整合するような認証データを生成することはできず、その結果、ユーザーＢによる契約内容の改ざんができない。

【００６６】さらに、前記認証データは契約内容を一方向性関数としてのハッシュ関数により変換したものであるため、仮に、契約後にユーザーＡが契約内容を改ざんしようとしても、ユーザーＢに与えた認証データと整合するようにユーザーＡが契約内容を改ざんすることも困難である。

【００６７】従って、前述のような認証データをユーザーＡからユーザーＢに与えることで、該ユーザーＡ，Ｂの両者にとって、契約の信頼性が強固なものとなる。

【００６８】また、契約に際しての両ユーザーＡ，Ｂ間の通信は、共通鍵K_{AB}あるいは乱数を鍵とした暗号通信によって行われるため、契約内容や認証データの部外者に対する機密性が確保される。この場合、前記乱数の暗号通信のための前記共通鍵K_{AB}は、各ユーザーＡ，Ｂが自身の端末装置１ａ，１ｂの共通鍵生成手段６に相手側の識別子を入力するだけで鍵管理局Ｃ等の関与を伴うことなく、生成することができ、また、最終的な契約内容や認証データの暗号通信を行うための鍵として使用する乱数は、ユーザーＢが自身の端末装置１ｂの乱数生成手段５により生成し、それを共通鍵K_{AB}により暗号化してユーザーＡの端末装置１ａに送信するだけで、ユーザーＡ，Ｂの両者で共有することができる。

16

【００６９】従って、両ユーザーＡ，Ｂは、契約のための通信を簡単に行うことができる。また、鍵管理局Ｃは、各ユーザＡ，Ｂ，…に共通鍵生成用アルゴリムや秘密鍵K_{AS}，K_{BS}，…を配付した後は、公開鍵方式の場合のような鍵の保守・管理等を行う必要がないため、該鍵管理局Ｃの負担は小さい。

【００７０】このため、本実施形態の電子契約を行うシステムを簡易で普及性の高いものとすることができる。

【００７１】次に本発明の第２の実施形態を図４を参照して説明する。尚、本実施形態は、前記第１の実施形態のものと、システム構成は同一であるので、構成部分については、図１及び図２の参照符号を用いて説明を省略する。

【００７２】図４を参照して、本実施形態では、二人のユーザーＡ，Ｂ間で、前記第１の実施形態と同様の契約を締結する場合、該第１の実施形態と全く同様に、ユーザーＡからユーザーＢへの契約の締結の意思表示と、これに続くユーザーＢからユーザーＡへの乱数（受諾側固有データ）の受け渡しとが行われる（ユーザーＡ側のＳＴＥＰ１ａ～ＳＴＥＰ３ａ及びユーザーＢ側のＳＴＥＰ１ｂ～ＳＴＥＰ３ｂ）。

【００７３】一方、ユーザーＢから乱数を受け取ったユーザーＡは、その端末装置１ａの契約処理システム９により、ユーザーＢと締結しようとする契約内容に固有で且つ該ユーザーＡに固有の認証データを次のように生成する。

【００７４】すなわち、ユーザーＡの端末装置１ａの契約処理システム９とユーザーＢの端末装置１ｂの契約処理システム９とは同一のハッシュ関数（一方向性関数）を有しており、ユーザーＡの端末装置１ａの契約処理システム９はユーザーＡから認証データの生成指示が与えられたとき、ユーザーＡがユーザーＢと締結しようとする契約内容を、まず、上記ハッシュ関数により変換する（ＳＴＥＰ４ａ）。

【００７５】尚、上記のようなハッシュ関数は、あらかじめ全てのユーザーＡ，Ｂ，…について同一として設定しておいてもよいが、例えば、それらのユーザー同士が契約を締結する際に使用する共通鍵K_{AB}，…や乱数をパ

ラメータとして契約の都度、設定するようにしてもよい。

【００７６】次いで、ユーザーＡの契約処理システム９は、ＳＴＥＰ４ａの変換により得られた変換データ（ハッシュ値）を、前記暗号・復号手段７によって、ユーザーＡの秘密鍵K_{SA}により暗号化せしめることで、認証データを生成する（ＳＴＥＰ６ａ）。この場合、前記変換データをユーザーＡの秘密鍵K_{SA}により暗号化して認証データを生成することで、該認証データは契約内容とユーザーＡとに固有のものとなる。

【００７７】このようにして、認証データを生成した後、ユーザーＡは、その認証データと、該認証データを生成する過程で得られた変換データと、これらの元文である契約内容とを、ＳＴＥＰ３ａで復号化して得た乱数を鍵として、暗号・復号手段７により暗号化し、その暗号化した認証データ、変換データ及び契約内容をユーザーＢの端末装置１ｂに送信する（ＳＴＥＰ５ａ）。

【００７８】また、暗号化された認証データ、変換データ及び契約内容を受信したユーザーＢは、その暗号化された認証データ、変換データ及び契約内容を、それぞれＳＴＥＰ３ｂで生成した乱数を鍵として、暗号・復号手段７により復号化することで、暗号化されていない本来の認証データ、変換データ及び契約内容を取得する（ＳＴＥＰ５ｂ）。そして、ユーザーＢはＳＴＥＰ５ｂで取得した契約内容と、前記ＳＴＥＰ２ｂで取得した契約内容とを照合し（ＳＴＥＰ６ｂ）、それらの内容の整合を確認する。

【００７９】さらに、ユーザーＢは、自身の端末装置１ｂの契約処理システム９によって、ＳＴＥＰ５ｂで取得した契約内容をユーザーＡ側と同一のハッシュ関数により変換し（ＳＴＥＰ７ｂ）、その変換により得られたデータと、ＳＴＥＰ５ｂで取得した変換データとを照合し（ＳＴＥＰ８ｂ）、両者のデータが一致しているか否かを確認する。

【００８０】そして、ＳＴＥＰ６ｂで契約内容の整合性が確認され、且つＳＴＥＰ８ｂで変換データの一致が確認されると、ユーザーＢはユーザーＡから与えられた契約内容に従ってユーザーＢとの契約を受諾する（ＳＴＥＰ９ｂ）。

【００８１】尚、ユーザーＡは、前記ＳＴＥＰ３ａで復号化した乱数や、ＳＴＥＰ５ａで暗号化する前の認証データ、変換データ及び契約内容を保管しておき、ユーザーＢは、ＳＴＥＰ３ｂで生成した乱数もしくはこの乱数の種とした一回性の数や、ＳＴＥＰ５ｂで復号化した認証データ、変換データ及び契約内容を保管しておく。

【００８２】このような本実施形態の電子契約によれば、ユーザーＢからユーザーＡへの乱数の受け渡しや、ユーザーＡからユーザーＢへの認証データの受け渡し等によって、前記第１の実施形態と同様の作用効果を奏することができる。

【００８３】さらに本実施形態では、ユーザーＡ側で認証データを生成する際に、契約内容をユーザーＢ側と同じハッシュ関数により変換してなる変換データをユーザーＡからユーザーＢに与え、ユーザーＢ側で、その変換データを確認することで、契約の信頼性をさらに高めることができる。すなわち、ユーザーＢ側で、ユーザーＡから送られてきた契約内容をハッシュ関数により変換してなるデータと、ユーザーＡから送られてきた変換データとが一致するということは、ユーザーＡが変換データを生成し、さらには認証データを生成する際の元文とした内容と、ユーザーＡがユーザーＢに送った契約内容とが一致することを意味する。従って、ユーザーＢ側で、ユーザーＡから送られてきた契約内容をハッシュ関数により変換してなるデータと、ユーザーＡから送られてきた変換データとを照合して、それらの一致を確認することで、ユーザーＢ側では、ユーザーＡが認証データを生成するに際して、正しい契約内容からハッシュ関数により変換データを生成したか否かを確認することができ、これにより、契約の信頼性をより一層高めることができる。

【００８４】次に、本発明の第３の実施形態を図５を参照して説明する。尚、本実施形態は、前記第１及び第２の実施形態のものと、システム構成は同一であるので、構成部分については、図１及び図２の参照符号を用いて説明を省略する。

【００８５】図５を参照して、本実施形態では、二人のユーザーＡ，Ｂ間で、前記第１及び第２の実施形態と同様の契約を締結する場合、該第１及び第２の実施形態と全く同様に、ユーザーＡからユーザーＢへの契約の締結の意思表示と、これに続くユーザーＢからユーザーＡへの乱数（受諾側固有データ）の受け渡しとが行われる（ユーザーＡ側のＳＴＥＰ１ａ～ＳＴＥＰ３ａ及びユーザーＢ側のＳＴＥＰ１ｂ～ＳＴＥＰ３ｂ）。

【００８６】一方、ユーザーＢから乱数を受け取ったユーザーＡは、その端末装置１ａの契約処理システム９により、ユーザーＢと締結しようとする契約内容に固有で且つ該ユーザーＡに固有の認証データを次のように生成する。

【００８７】すなわち、ユーザーＡは、ユーザーＢへの契約の申込みの日時を、前記第２の実施形態と同様にユーザーＢ側と同一のハッシュ関数を有する前記契約処理システム９に入力し、該契約処理システム９のハッシュ関数によって契約の申込みの日時を変換して成るタイムスタンプ（契約の申込みの日時に応じたデータ）を生成する（ＳＴＥＰ４ａ）。

【００８８】そして、ユーザーＡは、ＳＴＥＰ４ａで生成したタイムタンプと、ユーザーＢと締結する契約内容とを合わせたものを、契約処理システム９のハッシュ関数によって変換して、変換データ（ハッシュ値）を生成し（ＳＴＥＰ５ａ）、さらにその変換データを前記第２

の実施形態と同様に、ユーザーＡの秘密鍵K_{SA}により暗号化することで認証データを生成する（ＳＴＥＰ７ａ）。

【００８９】次いで、ユーザーＡは、契約内容と、タイムスタンプと、変換データと、認証データとを、ＳＴＥＰ３ａで復号化して得た乱数を鍵として、暗号・復号手段７により暗号化し、その暗号化した契約内容、タイムスタンプ、変換データ及び認証データをユーザーＢの端末装置１ｂに送信する（ＳＴＥＰ６ａ）。

【００９０】また、暗号化された契約内容、タイムスタンプ、変換データ及び認証データを受信したユーザーＢは、その暗号化された契約内容、タイムスタンプ、変換データ及び認証データを、それぞれＳＴＥＰ３ｂで生成した乱数を鍵として、暗号・復号手段７により復号化することで、暗号化されていない本来の契約内容、タイムスタンプ、変換データ及び認証データを取得する（ＳＴＥＰ５ｂ）。そして、ユーザーＢはＳＴＥＰ５ｂで取得した契約内容と、前記ＳＴＥＰ２ｂで取得した契約内容とを照合し（ＳＴＥＰ６ｂ）、それらの内容の整合を確認する。

【００９１】さらに、ユーザーＢは、自身の端末装置１ｂの契約処理システム９によって、ＳＴＥＰ５ｂで取得した契約内容とタイムスタンプとを合わせたものをユーザーＡ側と同一のハッシュ関数により変換し（ＳＴＥＰ７ｂ）、その変換により得られたデータと、ＳＴＥＰ５ｂで取得した変換データとを照合し（ＳＴＥＰ８ｂ）、両者のデータが一致しているか否かを確認する。

【００９２】そして、前記第２の実施形態と同様に、ＳＴＥＰ６ｂで契約内容の整合性が確認され、且つＳＴＥＰ８ｂで変換データの一致が確認されると、ユーザーＢはユーザーＡから与えられた契約内容に従ってユーザーＢとの契約を受諾する（ＳＴＥＰ９ｂ）。

【００９３】尚、ユーザーＡは、前記ＳＴＥＰ３ａで復号化した乱数や、ＳＴＥＰ５ａで暗号化する前の認証データ、変換データ及び契約内容と、タイムスタンプもしくは該タイムスタンプの元とした契約の申込みの日時とを保管しておき、ユーザーＢは、ＳＴＥＰ３ｂで生成した乱数もしくはこの乱数の種とした一回性の数や、ＳＴＥＰ５ｂで復号化した認証データ、変換データ、契約内容及びタイムスタンプを保管しておく。

【００９４】さらに、本実施形態では、ユーザＡ及びＢは、上記のように保管するデータを公証人Ｓに送って保管せしめる。この場合、各ユーザＡ，Ｂが公証人Ｓにデータを送るに際しては、それぞれ、公証人Ｓとの共通鍵K_{SA}，K_{SB}（＝各ユーザＡ，Ｂの秘密鍵）を使用した暗号通信によって、データを公証人Ｓに送る。

【００９５】このような本実施形態の電子契約によれば、ユーザーＢからユーザーＡへの乱数の受け渡しや、ユーザーＡからユーザーＢへの認証データの受け渡し等によって、前記第１の実施形態と同様の作用効果を奏することができる。さらに、前記第２の実施形態と同様に、ユーザーＢ側で、変換データの確認を行うことで、契約の信頼性を高めることができる。

【００９６】また、本実施形態では、変換データや認証データには、契約内容に加えて、ユーザーＡによる契約の申込みの日時が反映されるため、それらのデータは契約内容のみならず、ユーザーＡによる契約の申込みの日時にも固有のものとなり、それらのデータに基づく契約の信頼性がより強固なものとなる。特に、本実施形態では、契約の申込みの日時をそのまま使用して、変換データや認証データを生成するのではなく、該日時をハッシュ関数により変換した上で、それを変換データや認証データに反映させるため、例えばユーザーＡがユーザーＢに送ったタイムスタンプと整合するように契約の申込みの日時を偽ったりすることが困難であり、その結果、そのタイムスタンプがユーザーＡによる契約の申込みの日時を確定する上で有効なものとなる。

【００９７】さらに、本実施形態では、各ユーザーＡ，Ｂは、契約内容はもちろん、前記乱数もしくはその種である一回性の数、認証データ、変換データ、並びに、タイムスタンプもしくはその元となる契約の申込みの日時を公証人Ｓに送って保管せしめるので、ユーザーＡ，Ｂ間の契約の事実を確実なものとすることができる。

【００９８】尚、以上説明した各実施形態では、ユーザーＡ側で変換データや認証データを生成する際に、契約内容そのものを使用するようにしたが、該契約内容をユーザーＢから与えられた乱数を鍵として暗号化したものから、変換データや認証データを生成するようにしてもよい。このようにした場合には、前記変換データや認証データには、契約内容やユーザーＡに固有の秘密鍵K_{SA}だけでなく、ユーザーＢが生成したユーザーＢに固有の乱数も反映されるため、それらの変換データや認証データに基づく契約の効力を両ユーザーＡ，Ｂにとって、より強固なものとすることができる。

【００９９】また、前記第１及び第２の実施形態では、各ユーザーＡ，Ｂが乱数もしくはその種である一回性の数や、認証データ、変換データ等を前記第３の実施形態と同様に、公証人Ｓに送って保管せしめるようにしてもよい。

【０１００】また、前記各実施形態では、認証データを生成するための秘密鍵K_{SA}として、公証人Ｓとの共通鍵を使用するようにしたが、公証人Ｓとは無関係に各ユーザー毎に固有の秘密鍵を鍵管理局Ｃで生成して各ユーザーに配付しておくようにすることも可能である。但し、この場合には、公証人Ｓは、各ユーザーの秘密鍵を認証するためには、各ユーザーの秘密鍵を保管しておかなければならず、公証人Ｓの負担が大きい。これに対して、前記各実施形態のように、各ユーザーの秘密鍵として公証人Ｓの共通鍵を使用することで、公証人Ｓは自身が所持する共通鍵生成用アルゴリズムに各ユーザーの識別子

を入力することで、随時、各ユーザーの秘密鍵を生成することができ、該公証人Ｓの負担が極めて小さくて済む。

【０１０１】また、前記各実施形態では、受諾側固有データとして乱数を用いたが、例えば受諾側当事者（ユーザーＢ）の端末装置１ｂにおける入力操作の時刻を受諾側固有データとして用い、その時刻から申込み側当事者（ユーザーＢ）がデータの改ざんをできないような時間内で、該申込み側当事者に受諾側当事者への契約の申込みを行わせるようにしてもよい。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を適用した電子契約システムの全体的構成を示す説明図。

【図２】本発明の第１の実施形態において契約を行う当＊事者が所持する端末装置の機能的構成を示すブロック図。

【図３】本発明の第１の実施形態で契約を行う際の処理手順を示すフロー図。

【図４】本発明の第２の実施形態で契約を行う際の処理手順を示すフロー図。

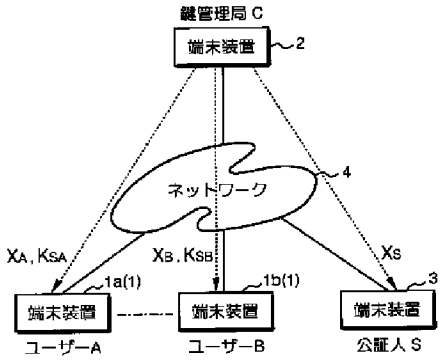
【図５】本発明の第３の実施形態で契約を行う際の処理手順を示すフロー図。

【符号の説明】

１（１ａ，１ｂ，…）…端末装置、Ａ，Ｂ…ユーザー（契約の当事者）、Ｓ…公証人（第三者）、K_{AB}…共通鍵、K_{SA}…秘密鍵、５…乱数生成手段、６…共通鍵生成手段、７…暗号・復号手段。

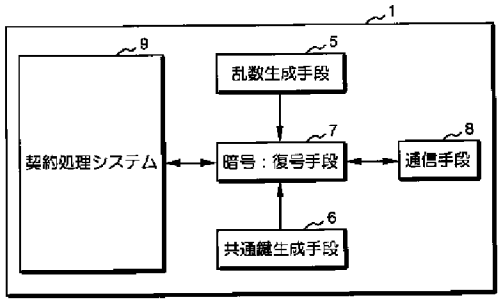
【図１】

FIG. 1



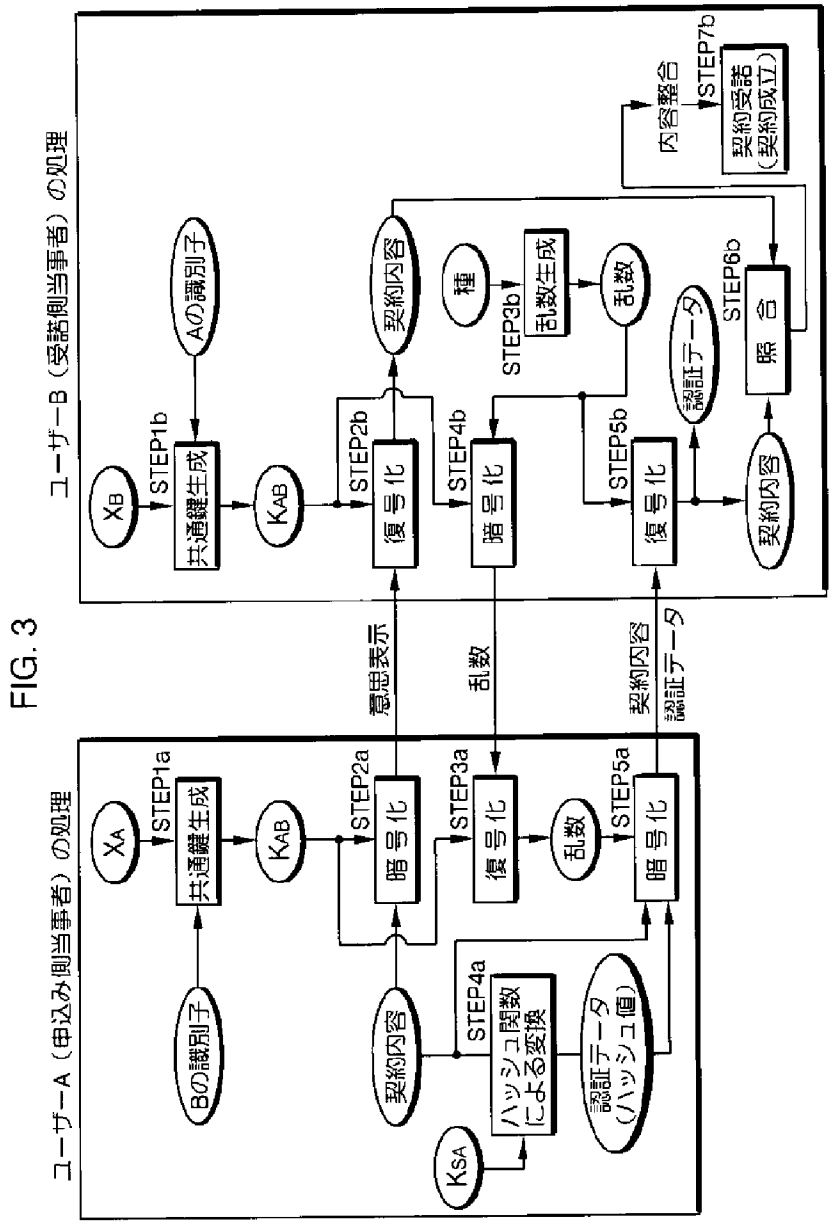
【図２】

FIG. 2



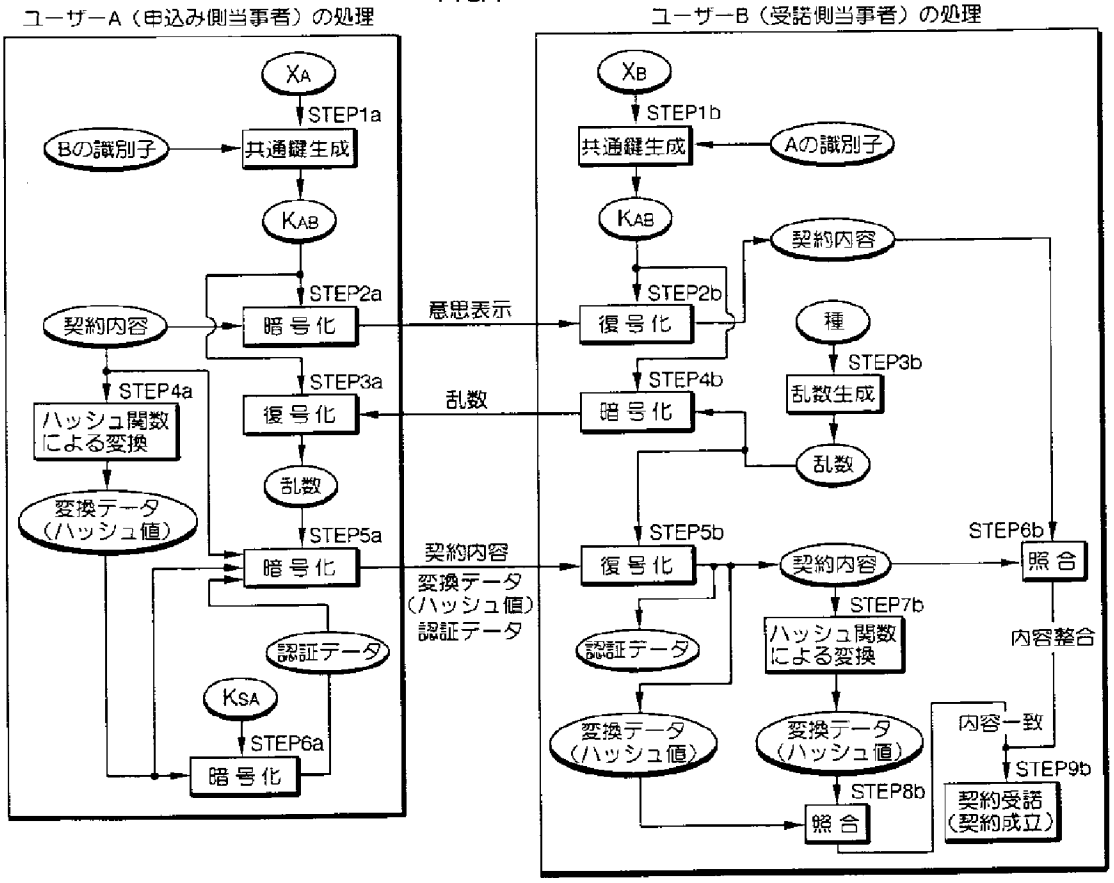
【図３】

FIG. 3


ユーザーA（申込み側当事者）の処理
ユーザーB（受諾側当事者）の処理
XA
XB
STEP1a
STEP1b
共通鍵生成
KAB
Bの識別子
Aの識別子
STEP2a
STEP2b
暗号化
復号化
契約内容
STEP3a
STEP3b
STEP4a
STEP4b
乱数生成
種
乱数
KSA
ハッシュ関数による変換
認証データ（ハッシュ値）
STEP5a
STEP5b
STEP6b
照合
内容整合
STEP7b
契約受諾（契約成立）
意思表示
乱数
契約内容
認証データ

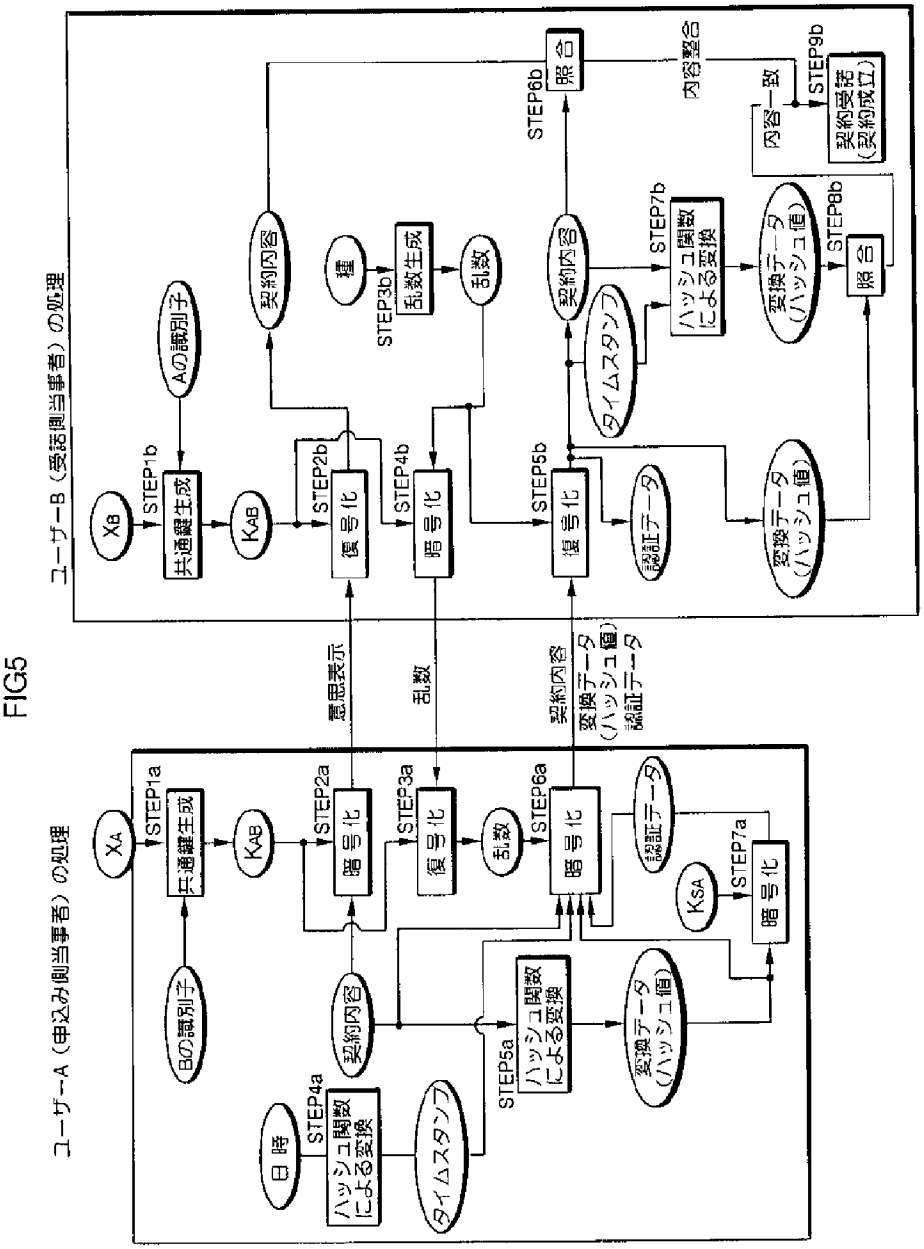
【図４】

FIG4


ユーザーA（申込み側当事者）の処理
ユーザーB（受諾側当事者）の処理
XA
STEP1a
Bの識別子
共通鍵生成
KAB
STEP2a
契約内容
暗号化
意思表示
STEP4a
ハッシュ関数による変換
STEP3a
復号化
乱数
変換データ（ハッシュ値）
乱数
STEP5a
暗号化
契約内容
変換データ（ハッシュ値）
認証データ
認証データ
KSA
STEP6a
暗号化
XB
STEP1b
共通鍵生成
Aの識別子
KAB
契約内容
STEP2b
復号化
種
STEP3b
乱数生成
STEP4b
暗号化
乱数
STEP5b
復号化
契約内容
STEP6b
照合
STEP7b
ハッシュ関数による変換
内容整合
認証データ
変換データ（ハッシュ値）
変換データ（ハッシュ値）
内容一致
STEP9b
STEP8b
照合
契約受諾（契約成立）

【図５】

FIG5


ユーザーA（申込み側当事者）の処理
ユーザーB（受話側当事者）の処理
XA
XB
KAB
KSA
STEP1a
STEP1b
共通鍵生成
Bの識別子
Aの識別子
日時
STEP4a
ハッシュ関数による変換
タイムスタンプ
契約内容
STEP2a
暗号化
STEP2b
復号化
意思表示
STEP3a
復号化
STEP4b
暗号化
乱数
種
STEP3b
乱数生成
STEP5a
ハッシュ関数による変換
変換データ（ハッシュ値）
STEP6a
暗号化
認証データ
契約内容
変換データ（ハッシュ値）
認証データ
STEP5b
復号化
STEP6b
照合
内容整合
内容一致
STEP9b
契約受諾（契約成立）
STEP7b
ハッシュ関数による変換
変換データ（ハッシュ値）
STEP8b
照合
STEP7a
暗号化